CHAPTER 13

Emerging Prudential Approaches to Enhance Banks' Cyber Resilience

Juan Carlos Crisanto and Jermy Prenio

13.1 Introduction

Cybercrime is a significant threat to the stability of the financial system and the global economy. The financial system performs a number of key activities that support the real economy (e.g. deposit taking and lending, payments and settlement services, wholesale funding). Cyber incidents have shown that these activities can be disruptive by affecting the information and communication technologies (ICT) that financial firms extensively rely on and the data they process. McAfee (2018) puts the annual cost of cybercrime to the global economy at around $600 billion while Accenture and Ponemon Institute (2019) estimates the global value at risk from cyber-attacks in 2019–2023 at approximately $5 Trillion. The latter report also finds that despite the significant efforts by the financial services industry to enhance cyber resilience, the average cost of cybercrime per financial firm is estimated to be $18.5 million (more than 40% higher than the average cost per company across all industries). In addition, the time required to resolve a cyber incident in financial

This paper is an updated version of *FSI Insights No 2*: "Regulatory approaches to enhance banks' cyber-security frameworks" by the same authors.

J. C. Crisanto · J. Prenio (✉)
Bank for International Settlements, Basel, Switzerland
e-mail: Jermy.Prenio@bis.org

J. C. Crisanto
e-mail: Juan-Carlos.Crisanto@bis.org

M. Pompella and R. Matousek (eds.), *The Palgrave Handbook of FinTech and Blockchain*, https://doi.org/10.1007/978-3-030-66433-6_13

firms has substantially increased (e.g. malware, up 89%; denial of service, up 63%). These developments reflect the evolving sophistication of cybercrime and the increasing availability of cyber-attack tools and methods at lower costs. The Covid-19 global lockdown has expanded the attack surface for cyber-threat actors and therefore created additional challenges in the quest to combat cybercrime.[1]

The Financial Stability Board (FSB 2018) defines cyber-risk as the combination of the probability of cyber incidents occurring and their impact. Cyber incidents are defined as events (whether resulting from malicious activity or not) that: (i) jeopardise the confidentiality, integrity and availability of an information system or the information the system processes, stores or transmits; or (ii) violate the security policies, security procedures or acceptable use policies.

The financial sector is arguably one of the sectors of the economy more exposed to cyber-risk given it is IT-intensive and highly dependent on information as a key input. Financial firms are also highly interconnected (including with other sectors) through the payment systems and provide products and services that are time-critical. Within the financial sector, banks typically have the most public-facing products and services. Bank systems' multiple points of contact with outside parties result in significant vulnerability to cyber-attacks, and could be used as entry points for attacks targeting other parts of the financial system.

In light of that, cyber resilience is a top priority for the financial services industry. The Deloitte's 2019 Global Risk Management Survey concluded the management of non-financial risks was assuming much greater importance at financial organisations and, among those, cybersecurity was a top concern. Moreover, close to 70% of respondents to the Deloitte's survey named cybersecurity as one of the three risks that would increase the most in importance for their business over the next two years, far more than for any other risk. Yet, only about one-half of the respondents felt their institutions were extremely effective or very effective in managing this risk.

Strengthening cyber resilience is a key area of attention for the official sector. Cybercrime is widely regarded as a national defence priority and a number of jurisdictions have put in place national policies or frameworks for strengthening the cybersecurity of critical sectors and institutions.[2] Central banks are developing analytical frameworks to understand the channels through which cyber-risk can grow from an operational disruption into a systemic event.[3] Bank supervisory authorities have come up with regulatory and supervisory frameworks to enhance the banking sector's resilience to cyber-attacks.

This paper presents the emerging regulatory and supervisory approaches to address banks' cyber resilience. First, the paper describes the international financial regulatory initiatives relevant for the regulation and supervision of cyber resilience. Second, it outlines the evolving approaches in the policy design of cyber resilience. Third, it presents the key regulatory requirements

implemented by banking authorities. Fourth, it explains the common supervisory frameworks and tools implemented around the world. Finally, the paper offers some policy considerations in implementing regulatory and supervisory approaches to enhance banks' cyber resilience frameworks.

13.2 International Regulatory Initiatives

Given the borderless nature of cybercrime and its potential impact to the global financial system, cyber resilience has become an important area for international cooperation among standard-setting bodies (SSBs) and financial authorities. FSB (2017) placed the need to mitigate the adverse impact of cyber-risk on financial stability among the top three priority areas for future international cooperation. To facilitate this cooperation through a common language, the FSB published a *cyber lexicon* in 2018 comprising a set of approximately 50 core terms related to cyber resilience in the financial sector. A key point of reference for the official sector continues to be the 2016 Committee on Payments and Market Infrastructures (CPMI) and the International Organization of Securities Commissions (IOSCO) *Guidance on cyber resilience for financial market infrastructures* published in 2016. Although the purpose of this document is to provide supplemental guidance for financial market infrastructures to enhance their cyber resilience, its core elements (particularly those related to governance and risk management) are widely accepted across the financial sector. The work on cyber resilience by the G7 finance ministers and central bank governors (the G7) is another common point of reference for the financial industry and the official sector community despite its non-binding nature. In this regard, the 2016 G7 *Fundamental elements of cybersecurity for the financial sector* (G7 FE) has played a pivotal role in providing private and public sector entities with building blocks to design and implement sound cybersecurity policies and practices. To assess the actual performance of these policies and practices, the G7 FE was followed in 2017 by the G7 *Fundamental elements for effective assessment of cybersecurity in the financial sector* (G7 FEA). In 2018, the G7 adopted two documents that further elaborate on its fundamental elements publication by providing financial entities with: (i) a guide to assess their resilience against cyber incidents by using simulated tactics, techniques and procedures of real-life threat actors (threat-led penetration testing); and (ii) best practices to effectively manage cyber-risks posed by third parties.[4]

In addition, SSB's work on cyber resilience has focused on: (i) enhancing a mutual understanding of their members' efforts by taking stock of their cybersecurity regulations, guidance and supervisory practices; and (ii) addressing different components of cyber resilience or its oversight. With respect to the former, an example is the 2018 Basel Committee on Banking Supervision (BCBS) report entitled *Cyber-resilience: Range of Practices* that describes and compares the range of regulatory and supervisory cyber resilience practices across BCBS member jurisdictions. Another relevant example is the

2019 Report from the IOSCO Cyber Task Force. This report examined how IOSCO member jurisdictions were using internationally recognised cyber frameworks and how these frameworks could help address any gaps identified in IOSCO members' current regimes rather than proposing any new guidance. Regarding the latter, the FSB issued a report in 2020 on *Effective practices for cyber incident response and recovery*, which proposes a toolkit to guide financial institutions to respond to and recover from a cyber incident in a way that limit any related financial stability risks. Another example is the work of the International Association of Insurance Supervisors (IAIS) through its 2018 *Application Paper on Supervision of Insurer Cybersecurity*. This document provides guidance to IAIS member authorities seeking to develop or enhance their approach to supervising the cyber resilience of insurers.

The cross-border nature of cyber-risk requires a high degree of alignment in national regulatory expectations. No single firm or regulator can successfully tackle cyber-risk alone. The above-mentioned G7 and SSBs work are facilitating a helpful level of convergence and therefore are steps in the right direction. However, there is still much work to do in this area. Differing regulatory frameworks for cyber-risk across jurisdictions could have the same impact as conflicting regulations or could inadvertently create regulatory gaps. For banks operating in various jurisdictions, alignment of regulatory expectations would help them avoid conflicting guidance, some of which would be undertaken simply for compliance purposes without any real improvement in cybersecurity.

13.3 Emerging Approaches for the Design of Cyber Resilience Policies

There are two extreme views on the regulation of banks' cyber-risk: one which sees no need for specific regulations, and the other which favours specific regulations. In the former, cyber-risk is viewed as any other risk and thus the general requirements for risk management (e.g. governance, setting of risk appetite, etc.), in particular IT, information security and operational risks, also apply. This view perceives the evolving nature of cyber-risk as not amenable to specific regulations, which would only become outdated and ineffective.[5] Regulations may also result in a compliance-based approach to dealing with cyber-risk. The latter view, on the other hand, emphasises the importance of providing structure through the regulation of cyber-risk in order to properly cope with its specificities and its growing relevance given the increasingly digitised nature of finance. In fact, specific regulations on cyber resilience are fairly recent and have been either introduced or proposed only in the last few years. In general, these are meant to supplement the more general regulations on IT, information security and operational risks.

One potential benefit of having specific regulations is that it can help ensure board and management buy-in. As regulation makes any issue more visible to boards and senior management, regulation on cyber-risk gives banks a stronger

incentive to continuously invest in improved cyber resilience. Banks' boards and senior management have the natural incentive to ensure sound cyber resilience given the potentially damaging monetary and reputational costs of cyber-attacks. However, boards and senior management may not always be forward-looking and may not appreciate the business implications of cyber-risk, and hence be inclined to subordinate cyber resilience to other business objectives in the absence of specific regulatory expectations.

However, the risk exists that specific regulations become too prescriptive, so that they fall behind both the constantly evolving threat from cyber-risk and advances in cyber-risk management. While prescriptive rules may be necessary in some areas, for example, by requiring banks' boards to establish a cyber-risk management framework and appetite, other areas are clearly less suitable for specific rules. Prescribing the use of a specific technology is one example; given the rate of technological change, any prescribed technology is likely to become rapidly outdated. Mandating a specific recovery time is another example where regulators need to be careful how banks go about implementing it. The aim is to prevent the lengthy disruption of critical financial operations, but an excessively stringent and rigid recovery time may prove counterproductive if this comes at the expense of banks' ability to thoroughly check that all their systems are no longer compromised.

In light of the trade-offs connected with issuing specific cyber regulations, there is an emerging regulatory approach that seeks to combine broad cyber resilience principles with a set of baseline requirements. This approach focuses more on "what expectations to achieve" and less on "how to achieve them."[6] It supports a regulatory framework that is flexible enough to be adjusted to the dynamic and evolving nature of cyber-risk while having clear supervisory expectations with respect to core aspects of governance and risk management that aim to enhance cyber resilience.

Regardless of the regulatory approach taken, the application of the proportionality principle should be given due consideration in the application of cyber resilience frameworks. Proportionality is defined as the application of simplified prudential rules to smaller and less complex banks to avoid excessive compliance costs without undermining key prudential safeguards.[7] Translating this concept to the cybersecurity world and considering that all banks are exposed to cybercrime, it would be important to identify key aspects of cyber resilience governance and risk management that should apply to all supervised firms regardless of their size, complexity and risk profile. At the same time, authorities should aim to have a clear idea about the extent to which systemically important banks and other institutions with a higher cyber-risk profile should be subject to heightened cyber resilience requirements.

Any cyber resilience framework should also be aligned with regulatory expectations on enterprise risk management and operational risk including operational resilience and ICT-related risks. A successful cyber-attack is very likely to affect people, processes and technology throughout a bank. At the

same time, sound operational risk management practices provide the foundation of a robust cyber resilience framework. As part of this, an effective response to and recovery from a cyber incident requires a sound operational resilience strategy. Therefore, it would be particularly challenging if cybersecurity were managed through its own set of responsibilities, policies and procedures, inconsistent with the overall risk management framework and operational risk approach. To mitigate this challenge, cyber-risk needs to be incorporated into the banks' enterprise-wide risk management framework and governance structure. Like any other bank risk, cyber-risk should be subject to the general risk management principles of risk identification, control, monitoring and mitigation. If necessary to help achieve this, supplemental guidelines may be issued applying or clarifying the application of the general risk management regulations to cyber-risk.

Existing technical standards on cyber and information security are a valuable point of reference for supervisory assessments of cybersecurity capabilities. For instance, the US National Institute of Standards and Technology (NIST) developed a cybersecurity framework in close cooperation with the private and public sectors. Consisting of a set of industry standards and best practices that help organisations manage cyber-risk, the framework is used voluntarily by organisations across the United States and has also received significant worldwide attention. As such, the NIST framework could be a valuable starting point for jurisdictions that decide to put in place or upgrade their approach to cybersecurity. Other influential technical standards in the cyber/information security community include the International Organisation for Standardisation and the International Electrotechnical Commission standards (in particular the ISO/IEC 27000 series on information security management, ISO 22301 on security and resilience and/or ISO 31000 on risk management); the Control Objectives for Information Technologies (COBIT) framework for IT governance and management; and the Center for Internet Security (CIS) Controls (which map into the NIST Framework). Relying on credible technical standards in which financial institutions may have already invested provides a solid foundation for any supervisory framework. Otherwise, adoption of supervisory assessment guidelines that differ considerably with existing technical standards could lead to confusing or conflicting approaches and result in unnecessary duplication of effort, leaving less resources for actual protection activities.

13.4 Key Regulatory Requirements Relating to Cyber Resilience

The tension between treating risks to cyber resilience the same as any other risks and the need for specific treatment given their significant implications has led to different regulatory approaches. This section discusses regulatory requirements and expectations in the area of cybersecurity strategy, governance and risk management; critical business services; cyber incident response and

recovery; cyber incident reporting and threat intelligence sharing; cybersecurity workforce and risk awareness; and third party dependencies.

13.4.1 Cybersecurity Strategy, Governance and Risk Management

Many regulators expect that banks' risk management frameworks and/or information security frameworks should cover risks to cyber resilience. As such, according to the 2018 BCBS report *Cyber-resilience: range of practices*, only a few regulators require banks to develop specific cybersecurity strategies that are separate from their information security strategies. For jurisdictions with specific regulatory requirements for cybersecurity strategies, the requirements typically follow the cybersecurity framework advocated in CPMI/IOSCO (2016) involving identification, protection, detection, response and recovery (see Fig. 13.1). Hence, these include general requirements on governance and oversight, risk ownership and accountability, information security or cyber hygiene measures (e.g. patch management procedures, access controls, identity management, etc.), periodic evaluation and monitoring of cybersecurity controls, incident response, business continuity and recovery planning.

Similarly, some regulators consider that existing general risk management frameworks already cover the roles and responsibilities of the board of directors (BoD) and senior management when it comes to addressing risks to cyber resilience. Other regulators, however, have issued specific regulatory guidance

Identification

- Baseline situation - threat profile, risk exposure and expected losses

Protection

- Increased third party security capabilities
- Internal and third party patches to ensure security and functionality of the application environment

Detection

- Assessment of applications' security capabilities
- Periodic scans for known security issues and vulnerabilities (vulnerability scans)
- Identification of vulnerabilities in network and physical security (penetration tests)
- Stealth assessment of organization's digital infrastructure and defenses (red team exercises)

Response

- Incident response capabilities across pre-determined threat scenarios (table top exercises)
- Dynamic simulation of a threat to assess incident response readiness and effectiveness (war gaming)

Recovery

- Stakeholders' response preparedness and effectiveness of business continuity plans
- Initiation of action plans and mobilization of resources to remediate following a cyber incident

Fig. 13.1 Emerging cybersecurity framework (*Sources* CPMI-IOSCO [2016]; Oliver Wyman's approach as described in Mee and Morgan [2017])

and requirements addressing such roles and responsibilities in the context of cyber resilience.

While most regulators do not require banks to implement the "three lines of defence" risk governance model,[8] specific regulatory guidance and requirements relating to roles and responsibilities in the context of cyber resilience commonly expect clear accountability within banks for cyber-related issues. These involve documented policies on clear assignment of cyber-related management responsibilities relating to identification, protection, detection, response and recovery. However, not many specifically require the designation of a Chief Information Security Officer (CISO) or equivalent. One possible reason is the lack of information security professionals who could fill this position. In fact, the requirement issued by the New York State's Department of Financial Services (DFSNY), for example, allows the CISO to be employed by a third-party service provider (i.e. not an employee) of the bank, subject to certain conditions.

Nevertheless, the designation of a CISO or equivalent is a common practice among large and globally active banks. The CISO oversees bank-wide cybersecurity. In some cases, the CISO reports to the Chief Risk Officer (CRO), in others to the Chief Information Officer (CIO). The former case would seem to be the natural choice since all of a bank's risks should be within the CRO's remit. However, CROs usually do not have a technology background and thus may not view cyber-risk as part of their remit, which may be narrowly defined as including only the traditional financial risks. In addition, some CROs might put more emphasis on compliance that might conflict with a CISO's approach of implementing cyber and IT security controls that still allow technological innovation. CIOs, on the other hand, are familiar with technology but their position in business operations creates a conflict with the review function of risk management (i.e. having the first and second lines of defence under one person or function). Given the importance of cyber resilience, there is a case to be made therefore for having CISOs report directly to the Chief Executive Officer (CEO) or the BoD.

13.4.2 Critical Business Services

Regulators generally expect banks to be able to identify their critical business services/operations. At the national level, governments identify critical infrastructure and firms to which their national cybersecurity frameworks apply. Banks are expected to do the same at their own level. Banks should be able to map their business services to their supporting assets (including third-party services), and be able to classify their business services according to their criticality and sensitivity to cyber-risk. This enables the prioritisation of cybersecurity efforts on assets that support critical business services. Ideally, the entire bank should be protected but, given limited resources, banks should be able to target where to deploy their resources to maximise the benefits and ensure operational resilience.

13.4.3 Cyber Incident Response and Recovery

Many regulators require banks to establish a framework for incident response and recovery. However, most requirements are not specific to cyber incidents with only a few regulators having cyber-specific business continuity and disaster recover requirements. Nevertheless, there is recognition that it is a question of when, not if, banks will experience a cyber-attack. This "assume breach" mentality is now replacing the traditional concept of building a strong perimeter to ward off a cyber-attack. The new threat environment, characterised by multiple points of potential entry for attacks, has reduced the effectiveness of the traditional security approach that relies solely on marshalling all of an institution's security devices/detective capability to guard the perimeter. The assumption of breach approach complements the traditional measures with intrusion detection techniques as well as response measures (e.g. to prevent the extraction of critical data).

To help financial institutions enhance their cyber incident response and recovery, FSB (2020) provides guidance in this area. The report provides a "toolkit" of 49 effective practices, structured across seven components:

Governance—frames how cyber incident and recovery is organised and managed.

Planning and preparation—to establish and maintain capabilities to respond to cyber incidents, and to restore critical functions, processes, activities, systems and data affected by cyber incidents to normal operations.

Analysis—to ensure effective response and recovery activities, including forensic analysis, and to determine the severity, impact and root cause of the cyber incident to drive appropriate response and recovery activities.

Mitigation—to prevent the aggravation of the situation and eradicates cyber threats in a timely manner to alleviate their impact on business operations and services.

Restoration and recovery—to repair and restore systems or assets affected by a cyber incident to safely resume business-as-usual delivery of impacted services.

Coordination and communication—to establish processes to improve response and recovery capabilities through lessons learnt from past cyber incidents and from proactive tools, such as tabletop exercises, tests and drills.

Improvement—to coordinate with stakeholders to maintain good cyber situational awareness and enhance the cyber resilience of the ecosystem.

13.4.4 Cyber Incident Reporting and Threat Intelligence Sharing

Cyber incident reporting by banks to regulators is a common regulatory requirement. Such reporting requirements have been established to achieve specific objectives, such as:

- Enable systemic risk monitoring of the financial industry by the regulator;

- Enhance or issue regulatory requirements/recommendations based on information collected;
- Allow appropriate oversight of incident resolution by regulators; and
- Facilitate further sharing of information with industry and regulators to develop a cyber incident response framework.

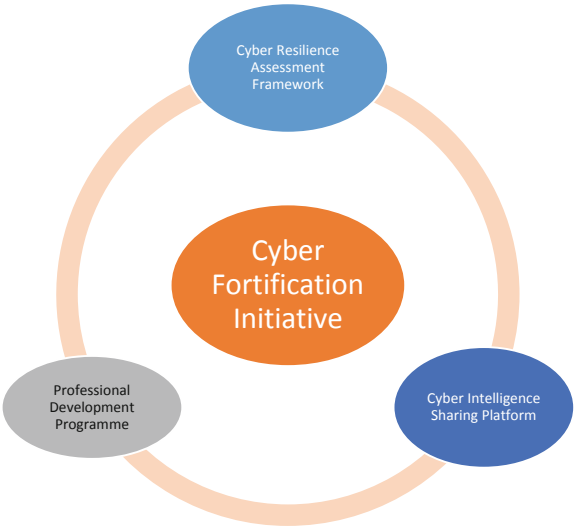
Some jurisdictions have specific requirements for the regulatory reporting of cyber incidents, subject to materiality (e.g. if the impact is deemed to be material enough to adversely impact the bank's operations) or the incident posing risk to a bank's critical business services. In other jurisdictions, cyber incidents are already captured in existing reporting requirements (e.g. events mandated by law or existing regulation to be reported to a government body or regulatory agency).[9] Moreover, there are different reporting frameworks ranging from formal communications to informal communications (e.g. free-text updates via email or verbal updates over the phone). In addition, there are differences in terms of taxonomy for reporting, reporting time frame (e.g. immediately, after two/four/72 hours after an incident), reporting templates and thresholds to trigger a report.

Cyber-threat intelligence sharing may not always be an explicit regulatory requirement, but it is encouraged and in most cases regulators play a role in facilitating the establishment of voluntary sharing mechanisms. Hong Kong is an example where regulations include an explicit requirement by incorporating in its Cyber Fortification Initiative (CFI) an element of effective infrastructure for sharing intelligence in which all banks are expected to participate (see Fig. 13.2). In other jurisdictions, while information-sharing may not be explicitly included in regulations, banks are "strongly encouraged" to participate in a sharing platform maintained by the authorities. In addition, banks may also be encouraged to participate in security information-sharing forums. Financial firms have also taken the initiative to establish their own efforts in this regard (e.g. through the Financial Services Information Sharing and Analysis Center (FS-ISAC)). In addition, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) has established a Customer Security Programme (CSP) that requires, among other things, that user institutions share all relevant information as soon as possible if they have been targeted or breached. This forms part of their contractual obligations as SWIFT users.

13.4.5 Cybersecurity Workforce and Risk Awareness

Some regulators have specific standards that address the responsibilities of the cybersecurity workforce and functions, with particular attention to training and competencies. In other cases, regulators certify the information security professionals used by banks for their cybersecurity activities. One reason for the need for regulatory certification is the sensitive nature of these activities, given that the people involved will gain insights into a bank's defences. The UK, for example, has established CBEST accreditation for any information security

The HKMA's Cybersecurity Fortification Initiative (CFI) has three main elements:



i. Cyber Resilience Assessment Framework – includes an inherent risk assessment, maturity assessment, and an intelligence-led cyber-attack simulation testing (iCAST);

ii. Professional Development Programme – seeks to increase supply of qualified cyber-security professionals in Hong Kong; HKMA is working with the HK Institute of Bankers and the HK Applied Science and Technology Research Institute (ASTRI) to develop a localised certification scheme and training programme for cyber-security professionals; and

iii. Cyber Intelligence Sharing Platform – seeks to provide an effective infrastructure for sharing intelligence on cyber-attacks; being set up by the HKMA together with the HK Association of Banks (HKAB) and ASTRI.

Fig. 13.2 The Hong Kong Monetary Authority's (HKMA's) cybersecurity fortification initiative (*Source* HKMA: Cybersecurity Fortification Initiative, 24 May 2016; graphic by FSI)

professionals involved in CBEST testing. This is in addition to the Council for Registered Ethical Security Testers (CREST) accreditation established by the industry. Another reason is the limited number of information security professionals in most jurisdictions. In Hong Kong, this is being addressed by including a Professional Development Programme (PDP) in its CFI. While the PDP is a local certification and training programme, its aim is to increase the supply of qualified cybersecurity professionals in the country. The scarcity of qualified people in this area is also reflected in the DFSNY regulation that allows banks to use cybersecurity professionals employed by third parties.

The problem, though, is not only about the limited availability of people with technical knowledge of cybersecurity. A further problem is the limited cybersecurity awareness of staff within banks, which itself could potentially open the way for a cyber incident. In essence, cybersecurity is less about technology and more about people (e.g. it is people, not computers, who click

on suspicious links). But there has been too much focus on technical solutions, and less so on people and processes. To address this, many regulators are encouraging the development of a common risk culture to ensure effective cybersecurity. Regulators have issued guidance and requirements emphasising the importance of risk awareness and risk culture for staff and management at all levels, including the BoD as well as third party employees. These include regulatory requirements relating to cybersecurity awareness training and cyber-related staffing. These also include measures to reduce the risk of theft, fraud or misuse of facilities (e.g. screening and background verification process for new employees, mandatory reverification process for existing employees at certain intervals, etc.).

13.4.6 Third-Party Dependencies

Third parties are widely used by banks to provide services, systems or IT solutions that support banks' operations. Traditionally, third parties relate to the providers of outsourc ed activities. In the cybersecurity context, third parties can be defined in a much broader sense to include products and services that are typically not considered as outsourc ed (e.g. power supply, telecommunication lines, hardware, software) as well as interconnected counterparties (e.g. payment and settlement systems, trading platforms, central securities depositories and central counterparties). These third parties may hold or may be able to access non-public information of banks and its customers. In addition, cybersecurity vulnerabilities in these third parties could become channels of attack on banks. The security capabilities of third-party service providers are therefore critical elements of any cybersecurity framework.

In most cases, regulators use outsourc ing regulations to address third-party dependencies. Outsourc ing regulations typically require either prior notification or authorisation of material outsourcing activities, the maintenance of an inventory of outsourced functions and reports on measurements of service level agreements (SLAs) and the appropriate performance of controls. Some outsourcing regulations also require sub-outsourcing activities to be visible to regulated entities so that they can manage the associated risks. In addition, outsourcing regulations generally require that banks develop management- and/or board-approved outsourcing and contractual frameworks that define banks' outsourcing policies and governance and specify obligations of the institution and the service provider in an outsourcing agreement, respectively.

In cases where there are regulatory expectations on broader third-party dependencies, regulators typically expect that banks take into account business continuity and information confidentiality and integrity. This is to ensure the availability of critical systems and the security of sensitive data that are accessible to, or held by, third party service providers. Regulations stress the importance of aligning business continuity plans of critical third-party providers (and their subcontractors) with the needs and policies of the bank in terms of business continuity and security. Confidentiality and integrity of

information, on the other hand, are addressed in general data protection requirements, contractual terms that are explicitly required to include confidentiality agreement, and security requirements for safeguarding the bank's and its customers' information.

A growing number of jurisdictions also have specific regulatory requirements for the use of the cloud by banks. These range from requiring information transferred to the cloud be subject to a contractual clause and that different cloud-specific issues be considered to ensure data security, to more specific requirements on data location, data segregation, data use limitations, data security and treatment of data in case of exit from the third party arrangement. For example, specific expectations for control and location of data are starting to emerge. These may take the form of requirements that the location of at least one data centre for cloud computing services provided in the country or region be identified, or data ownership, control and location be identified and monitored as part of the service agreement. Some jurisdictions further require a contractual clause that reserves the right for banks to intervene at, or give directives to, the service provider. However, commonalities in specific technical and operational requirements are still not emerging. Authorities seem to be emphasising different aspects of controls to ensure information confidentiality and integrity, ranging from explicitly requiring encryption solutions for confidential data to be under the banks' control, regulating the transfers of data abroad, to requiring explicit client consent for data handling by third parties.

13.5 Supervisory Frameworks and Tools

Most supervisors follow a more traditional approach and are assessing cybersecurity as part of their ongoing risk-based supervisory activities. This typically involves evaluating whether banks meet a series of criteria, which may be based on the banks' scale, complexity, business model and findings from previous on-site examinations. Supervisors then assign banks a rating or to a category and then, based on that rating or category, determine any management recommendations or supervisory actions. More recently, some supervisory authorities have used thematic or specialised reviews on cybersecurity as a complement to their supervisory work. In such cases, supervisors have internal guidance for identifying circumstances when they should conduct a specific cybersecurity review on a bank. The guidance typically looks at the bank's own risk assessments, previous on-site examinations findings, responses to questionnaires and cyber incidents.

Whether supervisors conduct reviews of cybersecurity as part of general risk management or independently, the reviews tend to focus on strategy, governance, cybersecurity capabilities including controls, monitoring, detection and response and recovery. While regulatory requirements and expectations described above inform supervisory reviews on a number of these areas, supervisors use specific frameworks or tools in certain cases.

13.5.1 Controls, Monitoring and Detection

Supervisors assess banks' cybersecurity controls, monitoring and surveillance of emerging threats, including real-time detection capability and ability to detect adversaries before they move between systems. These assessments are based on frameworks established in existing industry standards mentioned in Sect. 13.3, such as the NIST, ISO, COBIT and CIS frameworks.

13.5.2 Testing of Cybersecurity Capabilities

Supervisory assessments include a challenge on banks' approaches to testing controls and the remediation of issues identified. This can include a review of banks' responses to a supervisory questionnaire, audit reports and control testing reports that may be part of a more formal testing programme. The CPMI/IOSCO *Guidance on cyber resilience for financial market infrastructures*, which has provided a coherent approach to improving cyber resilience in financial institutions more broadly, called for the establishment of a comprehensive cyber resilience framework that includes a testing programme to validate the framework's effectiveness. Such a testing programme could employ various testing methodologies and practices, such as:

- Vulnerability assessment—systematic examination of an information system, and its controls and processes, to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures and confirm the adequacy of such measures after implementation.
- Penetration testing—a test methodology in which assessors, using all available documentation (for example, system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
- Red team testing (also referred to as threat-led penetration testing)—a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations.

While there is a range of testing methodologies and practices to validate an institution's cyber resilience capabilities, each with its own intended objective, there is recognition of the importance of red team testing. A number of jurisdictions have red team testing frameworks in place (see Table 13.1), although the objectives and implementation details may differ. The frameworks apply typically to large or critical financial institutions, but authorities may have discretion to include other financial institutions such as banks deemed risky from a supervisory perspective. The frameworks also differ in terms of whether

Table 13.1 Key information on red team testing frameworks in selected jurisdictions

Jurisdiction	*Framework*	*Year launched*	*Institutions covered*	*Threat intelligence and red team test providers*		
				External parties?	*Accreditation required?*	*Separate teams?*
European Union	Threat Intelligence-Based Ethical Red Teaming (TIBER-EU)	2018	At the discretion of relevant national or European authorities	Yes	No	Yes
Hong Kong SAR	Intelligence-led Cyber Attack Simulation Testing (iCAST)	2016	Banks that aim to attain "intermediate" or "advanced" maturity level are required; banks with "high" or "medium" inherent risk are expected	Not necessarily	No	Not necessarily
Netherlands	TIBER-NL	2016	Institutions that are part of the core financial infrastructure, plus larger insurance and pension fund providers	Yes	No	Yes
Saudi Arabia	Financial Entities Ethical Red-Teaming (FEER)	2019	All regulated financial institutions are encouraged but, as a minimum, domestic systemically important institutions are required	Yes	Yes	No
Singapore	Adversarial Attack Simulation Exercises (AASE)	2018	All financial institutions are encouraged but larger ones are expected	Not necessarily	No, but encouraged	Not necessarily
United Kingdom	CBEST	2014	Critical financial institutions are expected; non-critical ones may opt in	Yes	Yes	Yes

Source FSI Insights No 21: Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions

threat intelligence and red team test providers must be external to the financial institution, accredited and formally assessed.

Red team testing can strengthen institutions' cyber resilience posture by, among others, having a methodology to establish remediation plans to address identified weaknesses; being able to better organise and process threat intelligence; fostering closer cooperation among different units; promoting stronger security awareness and culture; and raising accountability of the BoD and senior management on cybersecurity. For supervisors, red team testing provides for a mechanism to understand better financial institutions' cyber resilience posture, as well as to identify common weaknesses and strengths across the industry. Nevertheless, there are challenges that need to be overcome, and certain facilitating conditions appear to be instrumental in supporting effective implementation of red team testing. Such conditions include a conducive governance structure, an engaged board of directors, a supportive risk culture and, critically, the availability of sound professional skills. A culture-related hurdle to overcome is getting firms and authorities to view a red team test as a "learn and improve" rather than a "pass or fail"

exercise. Other challenges in connection with red team testing include the high cost to firms, trust among the involved parties and data confidentiality.[10]

13.5.3 Cyber Incident Response and Recovery

Supervisory evaluation of banks' cyber incident response and recovery plans focuses on how plans are triggered, banks' ability to implement the plans, and preservation of data and critical systems. In addition, in some jurisdictions, supervisors conduct a review of post-incident learning. Supervisors usually conduct this review through discussion of banks' response and root cause analysis. Moreover, in many jurisdictions, supervisors and banks use exercises to train and practice how they would respond to a cyber incident. For example, there is an annual financial sector operational resilience exercise in the UK, which incorporates cyber-specific scenarios. In Japan, supervisors and banks conduct tabletop exercises to improve cybersecurity and, in particular, communication and coordination of response mechanisms.

13.5.4 Cybersecurity Workforce

Most supervisory authorities are in the early stages of implementing practices to monitor banks' cybersecurity workforce skills and resources. The range of supervisory practices includes assessment of staff expertise and background, assessment of staff training processes and assessment of adequacy of funding and resources to implement the bank's cybersecurity framework. Supervisors usually do these assessments during on-site examinations when they have the opportunity to talk with relevant cybersecurity specialists. Self-assessment questionnaires is also a common practice.

Attracting and retaining staff with cybersecurity expertise is also a key challenge for supervisory authorities. In 2015, the US Government Accountability Office reported that, while the country's largest deposit-taking institutions were generally examined by IT experts, medium and smaller institutions were sometimes reviewed by examiners with little or no IT training. According to the same report, US regulators recognised that, as some IT training is necessary for all examiners, efforts were under way to increase the number of staff with IT expertise and conduct more training. More generally, the 2017 Global Information Security Workforce Study, covering 2,620 cybersecurity professionals in the US federal government, reported that almost 70% of respondents indicated not having the staff necessary to address cyber threats, explaining that this was due mainly to difficulties in finding qualified personnel and retaining information security workers. The same study reports that the three most effective incentives for attracting and retaining cybersecurity staff are (i) offering training programmes or paying for security certification; (ii) improving compensation packages; and (iii) flexible work schedules.

13.5.5 Third-Party Dependencies

Supervisory approaches to assessing cyber-related risks of third-party dependencies follow the same approach as supervising outsourcing activities. Supervisors may conduct such assessments during on-site examinations by reviewing the outsourcing framework, the applicable processes and the completeness and adequacy of specific risk assessments and contracts. Supervisors may also conduct such assessment as part of their off-site monitoring activities. Supervisors receive periodic statements or reports that assess the outsourcing policies and risks at the financial institution. These reports will typically contain statements on the existence and adequacy of outsourcing policies, processes, risk assessments and contracts.

The ability to supervise third parties directly, however, depends on whether supervisory powers extend to third parties. Supervisors in most jurisdictions put the onus on banks to ensure that the third parties they deal with have the same stringent security policies, procedures and controls that the supervisors expect of regulated firms. Some supervisors have oversight of third parties and can therefore assess for themselves the soundness of cybersecurity in these firms,[11] while others require SLAs between banks and third parties to include a clause that allows supervisors to examine the latter's systems. In either case, supervisors have been using traditional supervisory tools in order to ensure that regulatory expectations are met. These include thematic off-site reviews based on self-assessment questionnaires as well as on-site examinations, on the basis of either formal requirements or authority or cooperation from third parties.

13.5.6 Cybersecurity and Resilience Metrics

Supervisors are still starting to develop metrics of the quality or level of cybersecurity and resilience of banks. The early metrics have focused on using information from reported incidents, surveys, testing activities and on-site inspections. However, none of these methodologies produce quantitative metrics or risk indicators comparable to those available for financial risks. Instead, these indicators provide broad information on banks' approach to building and ensuring cybersecurity and resilience. Moreover, a common drawback of the early methodologies is the tendency to focus on backward-looking indicators of the performance of the cybersecurity function. The nature of cyber-risk frustrates this approach because adversaries are dynamic and continuously adapt to responses and protective measures. There is an increasing recognition therefore of the need for forward-looking indicators as direct and indirect metrics of cybersecurity and resilience.

13.5.7 Cooperation and Collaboration Between Authorities

Supervisory cooperation and collaboration is important in dealing with cyber-related issues. Supervisors in different jurisdictions appear to be actively exchanging practices. Supervisors also share information on cyber-related issues involving supervised firms with other supervisors, be they domestic or cross-border, as appropriate according to established mandatory or voluntary information-sharing arrangements. Supervisors may also share such information through the many informal and ad hoc supervisory communication channels that exist, such as supervisory colleges and memoranda of understanding. Information shared may include regulatory actions, responses and measures.

In addition, jurisdictions have generally set out standards and practices for critical infrastructure and entities (including banks) and regulators to share cybersecurity information with national security agencies. While most jurisdictions adopt a voluntary approach, a few jurisdictions established formal sharing requirements. Computer Emergency Readiness Team (CERT) or similar security agencies may act as focal points for cyber incident notification in a jurisdiction.

13.6 Future Policy Considerations

Given the cross-border nature of cyber crime and its potential impact on the global financial system, SSBs and international financial authorities have been focusing their attention on enhancing international cooperation on cyber resilience. This has led to widely accepted building blocks for the design, enhancement and implementation of sound cyber resilience policies and practices such as the FSB cyber lexicon, the CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures and the G7 publications on fundamental elements of cybersecurity for the financial sector, threat-led penetration testing and third-party cyber risk management. These are steps in the right direction to achieve a higher degree of alignment in national regulatory expectations but much more needs to be done on international regulatory convergence in order to enhance global cyber resilience.

Another key point of reference for any supervisory framework are technical standards on cyber- and information security such as the NIST framework, the ISO standards, the COBIT framework and the CIS controls. Given the limited availability of resources in the field of cybersecurity, particularly in regulatory and supervisory agencies, existing technical standards on cyber- and information security are useful starting points for regulators and supervisors. This also avoids having duplicative and/or conflicting expectations when it comes to cybersecurity, which will only distract from banks' cybersecurity activities, as resources will have to be deployed to understand what each differing standard and guideline means.

In terms of policy design, there are two broad approaches to regulate cyber resilience: relying on general risk management expectations and, in particular, operational risk management, operational resilience and ICT-related regulations; or issuing specific regulations to deal with cyber-risk. Regardless of the approach taken, due consideration should be given to the proportional application of the cyber resilience framework. This means identifying core governance and risk management aspects of the framework that should apply to smaller and less complex financial institutions. Moreover, any cyber resilience framework should be aligned with the regulatory expectations on enterprise risk management and operational resilience. In light of the strong interconnections between those areas and cyber resilience, it would be beneficial to have consistency in their regulatory approaches.

There are common regulatory expectations emerging among jurisdictions that have opted for issuing specific cyber resilience regulations. Regulators generally follow the cybersecurity framework advocated in CPMI/IOSCO (2016) involving identification, protection, detection, response and recovery and typically expect clear accountability on those and other aspects of the cyber resilience framework. As part of this framework, regulators expect banks to identify and effectively manage their critical business/services and third-party dependencies. Although cyber incident reporting is also a common requirement, the specific technical and operational requirements seem to differ across jurisdictions. Another common regulatory expectation is establishing an incident response and recovery framework but a limited number of authorities appear to require a cyber-specific framework. One of the main objectives of the FSB toolkit on cyber incident response and recovery is to enhance public and private sector practices in this area.

A critical element of any regulatory framework is to promote cybersecurity awareness among staff. There is a tendency on the part of both regulators/supervisors and banks to focus too much on technical solutions. Often overlooked is the relevance of the human factor. Policies should encourage banks to develop a framework that enhances awareness among staff about cyber-risk and establishes metrics to measure this awareness. This approach is particularly relevant for smaller jurisdictions with limited resources and threat intelligence capabilities, as well as for dealing with smaller banks.

Most supervisors are assessing cybersecurity as part of their ongoing risk-based supervisory activities, while others are complementing these with thematic or specialised reviews. Regardless of the supervisory approach taken, these reviews tend to focus on strategy, governance, cybersecurity capabilities including controls, monitoring, detection and response and recovery. While regulatory requirements and expectations described above inform supervisory reviews on a number of these areas, supervisors use specific frameworks or tools in certain cases. To test an institution's cyber resilience capabilities, supervisors are increasingly using vulnerability assessment s, penetration testing, red team testing and other cyber resilience testing approaches. Despite the value

and different intended objectives of each of those testing approaches, there is growing recognition of the importance of red team testing.

It is necessary to explore further collaboration with the industry in strengthening banks' cybersecurity and to pursue greater cross-border cooperation. In some jurisdictions, regulators are working closely with the industry in creating or promoting platforms for intelligence sharing, developing a pool of cybersecurity professionals, and establishing guidelines on penetration testing. This could be a model that other jurisdictions could use, especially those with limited regulatory and supervisory resources, smaller banks, or a scarcity of cyber- and information security professionals. Moreover, given the scarcity of cybersecurity resources and the cross-border nature of cyber-risk, the need for supervisory cooperation cannot be overemphasised. In this regard, the BIS's Cyber Resilience Coordination Centre (CRCC) is expected to play a key role in facilitating cross-border cooperation. The CRCC seeks to provide a structured and careful approach to knowledge-sharing and collaboration between central banks in the area of cyber resilience. A core CRCC service is to provide a secure collaboration platform for information-sharing on multilateral cyber threats.

Notes

1. Crisanto and Prenio (2020).
2. For example, Singapore's Cybersecurity Strategy, Canada's Cybersecurity Standard, the US Department of Homeland Security's different initiatives to protect US critical infrastructure, South Africa's National Cybersecurity Policy Framework (NCPF); the Critical Infrastructure Protection in France.
3. For example, European Systemic Risk Board, Systemic Cyber Risk, February 2020; Bank of England, Could a Cyber Attack cause a Systemic Impact in the Financial Sector?, Q4 Quarterly Bulleting, 2018; US Office of Financial Research, Cybersecurity and Financial Stability: Risks and Resilience, February 2017. The academia is also actively involved in this area. See for example, Danielsson, J, Fouché, M and Macrae, R, Cyber Risk as Systemic Risk, 2016; Duffie, D. and Younger, J, Cyber Runs: How a Cyber Attack Could Affect U.S. Financial Institutions, 2019.
4. See G7 (2018a, b).
5. See Gracie (2014).
6. See Wilson et al. (2019).
7. See Castro Carvalho et al. (2017).
8. The "three lines of defence" risk governance model involves (1) business unit management as the first line; (2) independent risk management and compliance functions as the second line; and (3) an independent assurance function (internal and/or external audit) as the third line.
9. For example, the US Treasury Department's Financial Crime Enforcement Network (FINCEN) issued an Advisory on 25 October 2016 advising financial institutions to include cyber-related events in their Suspicious Activity Reports (SARs).
10. See Prenio et al. (2019) for more discussion on red team testing frameworks in different jurisdictions.

11. In the United States, the Bank Service Company Act (BSCA), 12 U.S.C. §1867(c) authorises the federal banking agencies to regulate and examine the performance of certain services by a third-party service provider for a depository institution "to the same extent as if such services were being performed by the depository institution itself on its own premises".

References

Accenture and Ponemon Institute. 2019. "The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study." March.

Bank of England. 2013. "CBEST Framework." June.

Basel Committee on Banking Supervision. 2018. "Cyber-Resilience: Range of Practices." December.

Castro Carvalho, Ana Paula, Stefan Holh, Roland Raskopf and Sabrina Ruhnau. 2017. "Proportionality in Banking Regulation: A Cross-Country Comparison." *FSI Insights No 1.* August.

Center for Cyber Safety and Education and International Information System Security Certification Consortium. 2017. "Global Information Security Workforce Study, US Federal Government Results." May.

Center for Internet Security. "The 20 CIS Controls & Resources." Accessed on 22 August 2020.

Committee on Payments and Market Infrastructures and International Organization of Securities Commissions. 2016. "Guidance on Cyber resilience for Financial Market Infrastructures." June.

Crisanto, Juan Carlos and Jermy Prenio. 2017. "Regulatory Approaches to Enhance Banks' Cybersecurity Frameworks." *FSI Insights No 2.* August.

———. 2020. "Financial Crime in Times of Covid-19 – AML and Cyber Resilience Measures." *FSI Briefs No 7*. May.

Deloitte. 2019. "Global Risk Management Survey, 11th Edition." January 23.

Department of Financial Services of New York State. 2017. "Cybersecurity Requirements for Financial Services Companies."

Financial Stability Board. 2017. "Financial Stability Implications from Fintech: Supervisory and Regulatory Issues that Merit Authorities' Attention." June 27.

———. 2018. "Cyber Lexicon." November 12.

———. 2020. "Effective Practices for Cyber Incident Response and Recovery, Consultative Document." April 20.

Gracie, Andrew. 2014. "Managing Cyber-Risk – The Global Banking Perspective." June 10.

Group of 7. 2016. "Fundamental Elements of Cybersecurity for the Financial Sector." May.

———. 2017. "Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector." May.

———. 2018a. "Fundamental Elements for Third Party Cyber Risk Management." October.

———. 2018b. "Fundamental Elements for Threat Led Penetration Testing." October.

Hong Kong Monetary Authority. 2016. "Cybersecurity Fortification Initiative." May.

International Association of Insurance Supervisors. 2018. "Application Paper on Supervision of Insurer Cybersecurity." November 7.
International Organization for Standardization. 2018. "ISO 31000: Risk Management."
———. 2019. "ISO 22301: Security and Resilience — Business Continuity Management Systems."
International Organization for Standardization and International Electrotechnical Commission. 2018. "ISO/IEC 27000: Information Technology — Security Techniques — Information Security Management Systems."
International Organization of Securities Commissions. 2019. "Cyber Task Force Final Report." June.
ISACA. 2019. "COBIT 2019 Framework: Introduction and Methodology."
McAfee. 2018. "The Economic Impact of Cybercrime – No Slowing Down." February.
Mee Paul and James Morgan. 2017. Deploying a cyber risk strategy: Five key moves beyond regulatory compliance, Oliver Wyman.
National Institute of Standards and Technology. 2018. "Cybersecurity Framework Version 1.1." April.
Prenio, Jermy, Jeffery Yong and Raymond Kleijmeer. 2019. "Varying Shades of Red: How Red Team Testing Frameworks Can Enhance the Cyber Resilience of Financial Institutions." *FSI Insights No 21.* November.
SWIFT. "Customer Security Programme (CSP)." Accessed on 20 August 2020.
US Government Accountability Office. 2015. "Cybersecurity, Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information." *Report to Congressional Requesters.* July.
Wilson, Christopher, Tamas Gaidosch, Frank Adelmann and Anastasiia Morozova. 2019. "Cybersecurity Risk Supervision." *IMF Monetary and Capital Markets Department Paper No19/15.* September.